Substitution: Recall in propositional logic $A(B/p_i)$

First-order: If $B \models\!\dashv C$, A^* is A w B replaced with C, then $A \models\!\dashv A^*$

Substitution of terms for variables x_i

Example: $\exists x_2 (x_2 + x_2 = x_1)$ "x_1 is even".

To say $x_3 + x_4$ is even, $\exists x_2 (x_2 + x_2 = x_3 + x_4)$

Notation A is $\exists x_2 (x_2 + x_2 = x_1)$

$A(x_3 + x_4 / x_1) - \exists x_2 (x_2 + x_2 = x_3 + x_4)$

Hodel uses $A_{x_1}[x_3 + x_4]$.

Warning: What if want to say $x_2 + x_3$ is even?

$A(x_2 + x_3 / x_1) = \exists x_2 (x_2 + x_2 = x_2 + x_3)$

does not say "$x_2 + x_3$" is even.

$\models \exists x_2 (x_2 + x_2 = x_2 + x_3)$

Fix #1: Use an "alphabetic variant" like $\exists x_5 (x_5 + x_5 = x_1)$

Fix #2 Define "substitutable for" – OK to substitute.

Notation: $A(t_1, \ldots, t_k / x_{i_1}, \ldots x_{i_k})$ means substitute "in parallel" each t_j for each free occurrence of x_{i_j}.

$A(\vec{t}/\vec{x})$ - shorthand notation.

Definition of substitution. Let s be a term. Let $t_1, \ldots, t_k$, $x_{i_1} \ldots x_{i_k}$ be as above. Then $s(\vec{t}/\vec{x})$ is recursively defined by:

(1) If s is x_{i_j}, then $s(\vec{t}/\vec{x})$ is t_j.

(2) If s is x_i, $i \notin \{i_1, \ldots, i_k\}$ or s is a constant symbol c, then $s(\vec{t}/\vec{x})$ is s.

(3) If s is $f(r_1, \ldots, r_l)$ - f is l-ary function, $s(\vec{t}/\vec{x})$ is $f(r_1(\vec{t}/\vec{x}), \ldots, r_l(\vec{t}/\vec{x}))$.

Let A be a formula.

(4) If A is atomic, i.e. A is $r_1 = r_2$ or $P(r_1, \ldots, r_l)$, P - l-ary then $A(\vec{t}/\vec{x})$ is $r_1(\vec{t}/\vec{x}) = r_2(\vec{t}/\vec{x})$, or $P(r_1(\vec{t}/\vec{x}), \ldots, r_l(\vec{t}/\vec{x}))$.

(5) If A is $\neg B$ or $B \circ C$ or $Qx_i\, B$, $i \notin \{i_1, \ldots, i_k\}$ Qx_i is $\forall x_i$ or $\exists x_i$ then $A(\vec{t}/\vec{x})$ is $\neg B(\vec{t}/\vec{x})$ or $B(\vec{t}/\vec{x}) \circ C(\vec{t}/\vec{x})$ or $Qx_i\,(B(\vec{t}/\vec{x}))$

(6) If A is $Qx_{i_j} B$ then $A(\vec{t}/\vec{x})$ is

$$Qx_{i_j}\, B(t_1, \ldots, t_{j-1}, t_{j+1}, \ldots t_k / x_{i_1}, \ldots x_{i_{j-1}}, x_{i_{j+1}}, \ldots x_{i_k}).$$

Defn t is substitutable for x_i in A is inductively defined by:

(1) If A is atomic, t is substitutable for x_i in A.

(2) If A is $\neg B$ or $B \circ C$ the t is substitutable for x in A iff t is substitutable for x in B, or in both B and C

(3) If A is $Qx_i B$, then t is substitutable for x_i in A.

(4) If A is $Qx_j B$, $j \neq i$, then t is substitutable for x_i in A iff either x_j does not occur in t or x_i is not free in B. (in A)

Informally t is substitutable for x_i in A iff there is no free occurrence of x_i in A, in the scope of a quantifier Qx_j such that x_j occurs in t.

Example $x_3 + x_4$ is substitutable for x_1 in $\exists x_2 (x_2 + x_2 = x_1)$

$x_2 + x_3$ is not substitutable " " " "

Theorem: (a) Let s be a term. t_j's terms, x_{i_j}'s - variables

$$\models x_{i_1} = t_1 \wedge \cdots \wedge x_{i_k} = t_k \to s = s(\vec{t}/\vec{x})$$

(b) If each t_j is substitutable for x_{i_j} in A, then

$$\models x_{i_1} = t_1 \wedge \cdots \wedge x_{i_k} = t_k \to (A \leftrightarrow A(\vec{t}/\vec{x}))$$

Pf - omitted -

Examples (1) $\models x = y \to x + z = y + z$

Take s to be $x + z$ $\quad s(y/x)$ is $y + z$.

(2) $\models x = y \to u = v \to x + u = y + v$

Take s to $x + u$, $\quad s(y, v/x, u)$ is $y + v$.

(3) For f - k-ary,

$$y_1 = z_1 \to y_2 = z_2 \to \cdots y_k = z_k \to f(y_1 \ldots y_k) = f(z_1 \ldots z_k).$$

Take s to $f(y_1 \ldots y_k)$ $\quad s(\vec{z}/\vec{y})$.

Equality Axioms

(4) $x = y \to (x \leq z \leftrightarrow y \leq z)$

Take A to be $x \leq z$ $\quad A(y/x)$ is $y \leq z$.

(5) $x = y \to u = v \to (x \leq u \leftrightarrow y \leq v)$. $\quad$ Take A to $x \leq u$.

⑥ $y_1 = z_1 \to y_2 = z_2 \to \cdots \to y_k = z_k \to (P(y_1 \ldots y_k) \leftrightarrow P(z_1, \ldots z_k))$

where P is k-ary

Equality Axioms.

Alphabetic Variants $\exists x_2 (x_2 + x_2 = x_1) \models\!\dashv \exists x_3 (x_3 + x_3 = x_1)$

Theorem Let $\exists x B$ be a formula.
Suppose y is substitutable for x in B and y does not appear free in B

then $\exists x B \models\!\dashv \exists y\, B(y/x)$.

Example B is $x_2 + x_2 = x_1$, x is x_2, $y = x_3$

Proof: $\models x = y \to (B \leftrightarrow B(y/x))$ by Previous Theorem.

$\mathfrak{M} \models \exists x B[\sigma] \iff \mathfrak{M} \models B[\tau]$ for some x-variant τ of σ.

$\iff \mathfrak{M} \models B[\pi]$ for the y-variant π of τ with $\pi(y) = \tau(x)$ since y not free in B

$\iff \mathfrak{M} \models B(y/x)[\pi]$ since $\pi(y) = \pi(x)$.

$\iff \mathfrak{M} \models \exists y B(y/x)[\pi]$

$\iff \mathfrak{M} \models \exists y\, B(y/x)[\sigma]$ since σ, π differ only in x and y and x, y not free in $\exists y\, B(y/x)$

QED

Informal notation for substitution.

Often write $A(x)$ and then later $A(t)$

to mean A is a formula (with free variable x that occurs only as indicated)

and $A(t)$ is $A(t/x)$.

Understood that t is substitutable for x in A

and there are no "extra" occurrences of x in A.

In structures, if $\mathfrak{A}$ is a structure and $a \in |\mathfrak{A}|$,

then $\mathfrak{A} \models A(a)$ means

$$\mathfrak{A} \models A[\sigma] \text{ for any } \sigma \text{ s.t. } \sigma(x) = a.$$

If A is $A(x_1 \ldots x_k)$

$\mathfrak{A} \models A[a_1 \ldots a_k]$ means $\mathfrak{A} \models A[\sigma]$

for any σ s.t. $\sigma(x_i) = a_i$ for all i.

Understood - use an alphabetic variant if necessary